(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－44992
（P2001－44992A）
(43)公開日　平成13年２月16日(2001.2.16)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	12/22		Ｈ０４Ｌ	11/26	
Ｇ０６Ｆ	15/00	３１０	Ｇ０６Ｆ	15/00	３１０Ａ
		３３０			３３０Ａ
	15/16	６２０		15/16	６２０Ａ
	15/177	６７０		15/177	６７０Ｃ

審査請求　未請求　請求項の数34　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願2000－148684(P2000－148684)

(22)出願日　平成12年５月19日(2000.5.19)

(31)優先権主張番号　０９／３１５６３６

(32)優先日　平成11年５月20日(1999.5.20)

(33)優先権主張国　米国（ＵＳ）

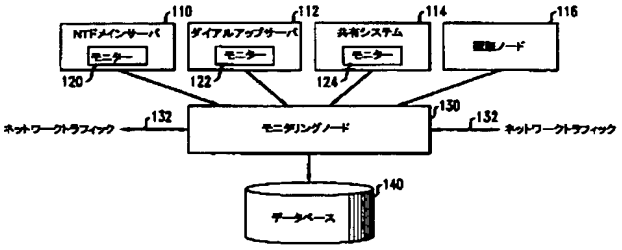
(71)出願人　596077259
ルーセント　テクノロジーズ　インコーポレイテッド
Ｌｕｃｅｎｔ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　Ｉｎｃ．
アメリカ合衆国　07974　ニュージャージー、マレーヒル、マウンテン　アベニュー　600－700

(74)代理人　100081053
弁理士　三俣　弘文

最終頁に続く

(54)【発明の名称】　ネットワーク動作方法、ネットワークノード、ネットワーク装置、及び通信ネットワーク

(57)【要約】
【課題】　データネットワークの利用状況を特定のユーザに関連付ける、より改善された技法を提供することが本発明の課題である。
【解決手段】　本発明に従って、ネットワークモニタリングノードがネットワーク認証ソースから認証データを受信する。認証データは、通常、認証済みユーザの識別及び当該ユーザに係る現時点でのネットワークアドレスを含んでいる。この認証データはモニタリングノードに蓄積される。その後、ネットワークアドレスを含むデータパケットの受信に応答して、モニタリングノードは、データパケットのネットワークアドレスをストアされたユーザのネットワークアドレスと比較することによって、ユーザをデータパケットに関連付ける。モニタリングノードは、ユーザの利用状況データを生成し、ユーザの利用状況データをデータベースに供給する。この利用状況データは、与えられたユーザに関して集積される。



1

【特許請求の範囲】

【請求項１】　ネットワークノードを動作させる方法において、当該方法が、ユーザをネットワークアドレスに関連付けるデータを少なくとも一つのネットワーク認証ソースから受信する段階；ここで、前記データはユーザの前記認証に即時応答して受信される；ネットワークアドレスを有するデータパケットを受信する段階；及び、前記ネットワークアドレスをユーザをネットワークアドレスに関連付ける前記データと比較することによって前記データパケットに関連付けられるユーザを実質的にリアルタイムで決定する段階；を有することを特徴とするネットワーク動作方法。

【請求項２】　前記方法が、さらに、前記データパケットに関連付けられるサービスを実質的にリアルタイムで決定する段階；を有することを特徴とする請求項１に記載のネットワーク動作方法。

【請求項３】　前記方法が、さらに、集積されるユーザ利用状況データをデータベースにストアする段階；を有することを特徴とする請求項１に記載のネットワーク動作方法。

【請求項４】　前記少なくとも一つの認証ソースが、認証サーバを含んでいることを特徴とする請求項１に記載のネットワーク動作方法。

【請求項５】　前記少なくとも一つの認証ソースが、設置された認証ノードを含んでいることを特徴とする請求項１に記載のネットワーク動作方法。

【請求項６】　少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する段階；ここで、前記ユーザ認証データはユーザの認証に即時に応答して受信される；データパケットを受信する段階；及び、ユーザを前記受信されたデータパケットに関連付ける目的で前記受信されたデータパケットを前記ユーザ認証データに対して実質的にリアルタイムで比較することによって利用状況データを生成する段階；を有することを特徴とするネットワーク動作方法。

【請求項７】　前記方法が、さらに、前記データパケットに関連付けられるサービスを実質的にリアルタイムで決定する段階；を有することを特徴とする請求項６に記載のネットワーク動作方法。

【請求項８】　前記方法が、さらに、集積されるユーザ利用状況データをデータベースにストアする段階；を有することを特徴とする請求項６に記載のネットワーク動作方法。

【請求項９】　前記方法が、さらに、前記データパケットに関連付けられた前記ユーザに依存して前記データパケットを相異なった方式で処理する段階；を有することを特徴とする請求項６に記載のネットワーク動作方法。

【請求項１０】　前記方法が、さらに、前記利用状況データに基づいてユーザに課金する段階；を有することを特徴とする請求項６に記載のネットワーク動作方法。

2

【請求項１１】　前記方法が、さらに、前記利用状況データに基づいてネットワークサービス品質を実現する段階；を有することを特徴とする請求項６に記載のネットワーク動作方法。

【請求項１２】　ネットワーク利用状況データを生成する方法において、当該方法が、少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する段階；ここで、前記ユーザ認証データはユーザの認証に即時に応答して受信される；ネットワークトラフィックをモニタする段階；及び、前記ネットワークトラフィックを前記ユーザ認証データと比較することによって前記ネットワークトラフィックのある部分を特定のユーザに対して実質的にリアルタイムで関連付ける段階；を有することを特徴とするネットワーク動作方法。

【請求項１３】　前記方法が、さらに、前記ネットワークトラフィックのある部分を特定のサービスに対して実質的にリアルタイムで関連付ける段階；を有することを特徴とする請求項１２に記載のネットワーク動作方法。

【請求項１４】　前記方法が、さらに、集積されるユーザ利用状況データをデータベースにストアする段階；を有することを特徴とする請求項１２に記載のネットワーク動作方法。

【請求項１５】　前記方法が、さらに、前記ネットワークトラフィックの前記部分に関連付けられた前記ユーザに依存して前記ネットワークトラフィックの前記部分を相異なった方式で処理する段階；を有することを特徴とする請求項１２に記載のネットワーク動作方法。

【請求項１６】　前記方法が、さらに、前記ネットワーク利用状況データに基づいてユーザに課金する段階；を有することを特徴とする請求項１２に記載のネットワーク動作方法。

【請求項１７】　前記方法が、さらに、前記ネットワーク利用状況データに基づいてネットワークサービス品質を実現する段階；を有することを特徴とする請求項１２に記載のネットワーク動作方法。

【請求項１８】　少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する目的；ここで、前記ユーザ認証データはユーザの認証に即時に応答して受信される；及び、ネットワークトラフィックを受信する目的；で使用される少なくとも一つのネットワークインターフェース；前記受信されたユーザ認証データをストアするメモリ；及び前記ネットワークトラフィックのある部分を特定のユーザに関連付ける目的で前記ネットワークトラフィックを前記ストアされたユーザ認証データと実質的にリアルタイムで比較するように、ストアードプログラムコードに従って動作するプロセッサ；を有することを特徴とするネットワークノード。

【請求項１９】　前記プロセッサが、さらに、ストアードプログラムコードに従って前記ネットワークトラフィックのある部分に関連付けられたサービスを実質的にリ

アルタイムで決定するように機能すること；を特徴とする請求項１８に記載のネットワークノード。

【請求項２０】　ネットワーク利用状況データ生成装置において、当該装置が、少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する手段；ここで、前記ユーザ認証データはユーザの認証に即時に応答して受信される；ネットワークトラフィックをモニタする手段；及び、前記ネットワークトラフィックを前記ユーザ認証データと比較することによって前記ネットワークトラフィックのある部分を特定のユーザに対して実質的にリアルタイムで関連付ける手段；を有することを特徴とするネットワーク装置。

【請求項２１】　前記装置が、さらに、前記ネットワークトラフィックのある部分を特定のユーザに実質的にリアルタイムで関連付ける手段；を有することを特徴とする請求項２０に記載のネットワーク装置。

【請求項２２】　前記装置が、さらに、集積される利用状況データをデータベースにストアする手段；を有することを特徴とする請求項２０に記載のネットワーク装置。

【請求項２３】　ユーザがデータを送受信する目的で利用する通信ネットワークにおいて、当該ネットワークが、

１）ユーザ認証に即時応答してユーザ認証データを送信する少なくとも一つのネットワーク認証ソース；及び、

２）ａ）ユーザ認証データを少なくとも一つのネットワーク認証ソースから受信する目的；及びデータネットワークトラフィックを受信する目的；で用いられる少なくとも一つのネットワークインターフェース；

ｂ）前記受信されたユーザ認証データをストアするメモリ；及び、

ｃ）前記ネットワークトラフィックのある部分を特定のユーザに関連付ける目的で前記ネットワークトラフィックを前記ストアされたユーザ認証データと実質的にリアルタイムで比較することによってユーザ利用状況データを生成するプロセッサ；を有することを特徴とする通信ネットワーク。

【請求項２４】　前記通信ネットワークが、さらに、集積されるユーザ利用状況データをストアするデータベース；を有することを特徴とする請求項２３に記載の通信ネットワーク。

【請求項２５】　前記通信ネットワークが、さらに、前記ユーザ利用状況データを受信し、利用状況に少なくとも一部分基づいてユーザに課金する課金アプリケーション；を有することを特徴とする請求項２３に記載の通信ネットワーク。

【請求項２６】　前記通信ネットワークが、さらに、前記ユーザ利用状況データを受信し、前記ユーザ利用状況データに少なくとも一部分基づいてユーザに対してサービス品質を提供するサービス品質アプリケーション；を

有することを特徴とする請求項２３に記載の通信ネットワーク。

【請求項２７】　前記通信ネットワークが、さらに、前記ユーザ利用状況データを受信し、前記ユーザ利用状況データに少なくとも一部分基づいてネットワークトラフィックを制限するファイアウォール；を有することを特徴とする請求項２３に記載の通信ネットワーク。

【請求項２８】　ユーザがデータを送受信する目的で利用する通信ネットワークにおいて、当該ネットワークが、

１）ユーザによるデータ転送の開始に即時応答してユーザ認証データを生成かつ送信するプログラムコードを有するソケットライブラリを有する、複数の同時ユーザを有する共用コンピュータシステム；

２）ａ）ユーザ認証データを前記共用コンピュータシステムから受信する目的；及びデータネットワークトラフィックを受信する目的；で用いられる少なくとも一つのネットワークインターフェース；

ｂ）前記受信されたユーザ認証データをストアするメモリ；及び、

ｃ）前記ネットワークトラフィックのある部分を特定のユーザに関連付ける目的で前記ネットワークトラフィックを前記ストアされたユーザ認証データと実質的にリアルタイムで比較することによってユーザ利用状況データを生成するプロセッサ；を有することを特徴とする通信ネットワーク。

【請求項２９】　ユーザによるデータ転送の開始に即時応答して共用コンピュータシステムからユーザ認証データを受信する段階；データパケットを受信する段階；及び、ユーザを前記受信されたデータパケットと関連付ける目的で前記受信されたデータパケットを前記ユーザ認証データと実質的にリアルタイムで比較することによって利用状況データを生成する段階；を有することを特徴とするネットワーク動作方法。

【請求項３０】　前記方法が、さらに、前記データパケットに関連付けられたサービスを実質的にリアルタイムで決定する段階；を有することを特徴とする請求項２９に記載のネットワーク動作方法。

【請求項３１】　前記方法が、さらに、集積される利用状況データをデータベースにストアする段階；を有することを特徴とする請求項２９に記載のネットワーク動作方法。

【請求項３２】　前記方法が、さらに、前記データパケットに関連付けられたユーザに基づいて前記ネットワークにおける前記データパケットを相異なった方式で処理する段階；を有することを特徴とする請求項２９に記載のネットワーク動作方法。

【請求項３３】　前記方法が、さらに、前記利用状況データに基づいてユーザに課金する段階；を有することを特徴とする請求項２９に記載のネットワーク動作方法。

5

【請求項３４】　前記方法が、さらに、前記利用状況データに基づいてネットワークサービス品質を提供する段階；を有することを特徴とする請求項２９に記載のネットワーク動作方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータネットワークに関し、特に、ネットワークの利用を特定のユーザに関連付ける技法に関する。

【０００２】

【従来の技術】歴史的には、データネットワークに係るユーザ固有の利用状況に関するデータの収集は、ネットワーク設計者の主たる対象ではなかった。例えば、インターネットの利用は伝統的はユーザに対して無料であり、実際の費用は種々の研究機関、企業、及び政府関係機関の予算に吸収されてきた。よって、ネットワークのモニタリング及びプランニングに関して大量のネットワーク利用状況データが集積されてきたにもかかわらず、ユーザ固有のネットワーク利用状況情報を収集する必要はほとんど無かった。

【０００３】しかしながら、一般的に言えばデータネットワーク、特にインターネットが成長して発展するに連れ、ユーザ固有の利用状況情報に係る必要性が生じてきている。この必要性はいくつかの要因に関連付けられる。第一に、ネットワーク事業者は、ネットワークサービスの提供に係るコストを回収する方法を必要としている。現在の利用無制限の一様な利用料金方式は、より多くの革新的かつ差別化されたサービスを提供する際の障害になっている。従来技術に係る音声電話ネットワークにおいて用いられてきたような、利用状況に基づくより身近な料金モデルを採用することにより、サービスプロバイダが革新的なサービスを提供すること及びそれに従って課金することが可能になる。

【０００４】第二に、サービス品質に係る要求の増大は利用状況に基づく情報の必要性を示唆している。伝統的には、データネットワークはベスト・エフォートというサービスポリシーの下で運営されており、全てのネットワークユーザのデータトラフィックには同一の優先度が与えられてきた。しかしながら、保証されたサービス品質に対する弁済を希望するユーザが増大しつつある。よって、相異なったユーザに係るデータトラフィックを弁別することが可能であることへの要求が存在する。

【０００５】第三に、企業はその内部のデータネットワーク（すなわちイントラネット）に対するかなりの投資を行なっており、それらのネットワークの利用状況をより詳細にモニタする方法を求めている。この種の利用状況情報は、課金、ネットワークプランニング、及びネットワーク資源の悪用の発生可能性の制御に係る基礎となりうる。

【０００６】現在のデータネットワークにおけるユーザ

6

の利用状況に係る一つの問題点は、データネットワークを介して伝達されるデータパケットが当該データパケットを送受信するユーザを識別しない、という点である。その代わり、データパケットは、データパケットが送出元の機械のアドレス（ソースアドレス）及びデータパケットの送出先の機械のアドレス（デスティネーションアドレス）を識別する。公知のインターネットプロトコル（ＩＰ）に従って機能させられているネットワークにおいては、これらのアドレスはＩＰアドレスと呼称される。ＩＰアドレスは、一般に、種々の理由から特定のユーザに対してマッチングされることは不可能である。この種の理由の一つは、ＩＰアドレスがしばしば動的に割り当てられ、その結果、特定の機械のアドレスがその機械がデータネットワークに登録されるたび毎に変化する可能性がある、というものである。別の問題は、機械が固定ＩＰアドレスを有している場合においても、あらゆる時刻において、複数のユーザがデータネットワークへのアクセス目的で同一機械を用いうる、ということである。

【０００７】

【発明が解決しようとする課題】ユーザ固有の利用状況に基づく情報を提供するために種々の試みがなされている。それらの試みの一つはＲＡＤＩＵＳプロトコルであり、これは認証であって、ＲＡＤＩＵＳサーバとダイアルインネットワークアクセスサーバとの間での通信に関して用いられる認証課金プロトコルである。加入者が、認証にＲＡＤＩＵＳプロトコルを用いるネットワークアクセスサーバにダイアルする際、サービスプロバイダはそのダイアルインセッションの間のその特定のユーザによる利用状況を追跡することが可能となる。ユーザはＲＡＤＩＵＳサーバによって認証されたため、サーバはユーザの識別及びそのダイアルアップセッションにおいてそのユーザ宛に割り当てられたＩＰアドレスの双方を知っていることになる。さらに、ユーザがネットワークアクセスサーバを介してデータネットワークに接続されているため、そのユーザに係る全てのデータトラフィックはネットワークアクセスサーバを経由しなければならない。よって、利用可能なデータを組み合わせることによって、サービスプロバイダはユーザ固有の利用状況データを追跡することが可能となる。それ以前の技法に関する明らかな改善はあるものの、ＲＡＤＩＵＳプロトコルはサービスプロバイダのシステムに対してダイアルアップする加入者に係るそのダイアルアップセッションの間だけのユーザ利用状況を追跡することができるのみである。ＲＡＤＩＵＳプロトコルに関するさらなる情報は、例えば、C.Rigneyらによる“リモート認証ダイアルインユーザサービス（ＲＡＤＩＵＳ）”（ＩＥＴＦネットワークワーキンググループのＲＦＣ２１３８、１９９７年４月）；及び、C.Rigneyによる“ＲＡＤＩＵＳ課金”（ＩＥＴＦネットワークワーキンググループのＲＦＣ２

１３９、１９９７年４月）より得られる。

【０００８】用いられている他の技法は、種々のネットワークロケーションにおいて収集されたデータの相関である。現在では、多くのネットワークノードは、監査、セキュリティ、及び課金などの目的のために利用状況ログを記録する。例えば、シスコシステムズ社（Cisco Systems, Inc.）より市販されているＮｅｔＦｌｏｗという製品は、ルータ及びスイッチなどのネットワークノードにおける利用状況ログを記録するソフトウエアコンポーネントである。ＮｅｔＦｌｏｗは、ＩＰアドレス間のデータパケットフローを記録し、さらに、データパケットがノードによって処理される時間間隔も記録する。同様に、Microsoft NTドメインサーバやＲＡＤＩＵＳサーバなどのネットワーク認証デバイスは、ユーザによるネットワークに対するログオン及びログオフに係る認証ログを生成する。これらの認証ログは、ユーザＩＤ、セッションの間にユーザＩＤに対して割り当てられたＩＰアドレス、及びユーザがシステムに対してログオン及びログオフした時刻を含んでいる。利用状況ログ及び認証ログが集中的に収集される場合には、これらログに含まれる情報の相関を調べることによって、ユーザに係る利用状況を再生成することが可能である。しかしながら、この技法にはいくつかの欠点が存在する。第一に、データが複数の異種ソースより収集されなければならないため、データ収集が複雑である。第二に、双方のログシステムの同期が取られていない場合には、利用状況を特定のユーザに関連付けることが困難あるいは不可能である。第三に、同一のネットワークトラフィックに係る複数の利用状況記録が収集される可能性があって、利用状況の二重測定になる可能性がある。

【０００９】インターネット課金に係る技法は、R. Edell、N. McKeown、及びP. Varaiyaにｙる“ＴＣＰに係るユーザ課金及び価格”という表題の論文（IEEE Journal on Selected Area in Communications、第１３巻第７号、１９９５年９月）に記載されている。記載されている技法は、接続指向インターネットトラフィックに係るユーザの利用状況を測定する。接続指向トラフィックとは、あらゆるデータトラフィックが送出される前に、二台の機械の間の接続が設定されなければならないことを意味している。ゲートウェイは、接続設定要求を認識すると、当該接続に係るユーザを識別するため、その接続を介したトラフィックを識別されたユーザに関連付けることが可能になる。この方式の一つの問題点は、ゲートウェイがユーザの認識を指向する間、接続設定が遅延させられることである。この方式に係る別の問題は、この方式が接続指向通信（例えば、ＴＣＰプロトコル）に関してのみ有効であるということである。この方式は、接続なし通信（例えば、ＵＤＰプロトコル）に関しては機能しない。

【００１０】よって、データネットワークの利用状況を特定のユーザに関連付ける、より改善された技法に関する要求が存在する。

【００１１】

【課題を解決するための手段】本発明は、ネットワークトラフィックを特定のユーザに対して実質的にリアルタイムで関連付ける方法を提供する。

【００１２】本発明に従って、ネットワークモニタリングノードは、ネットワーク認証ソースから認証データを受信する。認証データは、通常、認証済みユーザの識別及び当該ユーザに係る現時点でのネットワークアドレスを含んでいる。この認証データはモニタリングノードに蓄積される。その後、ネットワークアドレスを含むデータパケットの受信に応答して、モニタリングノードは、データパケットのネットワークアドレスをストアされたユーザのネットワークアドレスと比較することによって、ユーザをデータパケットに関連付ける。モニタリングノードは、ユーザの利用状況データを生成し、ユーザの利用状況データをデータベースに供給する。この利用状況データは、与えられたユーザに関して集積される。

【００１３】本発明の一実施例に従って、ネットワーク認証ソースのうちの少なくとも一つが、ネットワークに接続するユーザを認証するネットワーク認証サーバとなる。ネットワーク認証サーバは、ユーザの認証に即時に応答して、認証データを生成してモニタリングノード宛に送出する。本発明の別の実施例においては、ネットワーク認証ソースのうちの少なくとも一つが、複数の同時ユーザを有する共用コンピュータである。共用コンピュータは、ユーザによるデータ転送の開始に即時に応答してユーザ認証データを生成してモニタリングノード宛に送出するコンピュータプログラムコードを有するソケットライブラリを含むように配置されている。

【００１４】本発明の一実施例に従って、モニタリングノードは、受信されたデータパケットに係るサービス、すなわちサービス品質の決定をも行なうことが可能である。

【００１５】有利なことには、本発明は、ユーザレベルにおいてリアルタイムサービスを提供する目的で、種々のネットワークアプリケーションと共に用いられうる。このようなサービスは、従来技術においてはユーザレベルで提供され得なかったものである。例えば、本発明は、ユーザレベル課金システム、ファイアウォール、ゲートウェイ、プリペイドサービス、ネットワークポリシー強制、及びサービス品質モニタリングなどを実装する目的で用いられうる。

【００１６】本発明に係る上記及びその他の利点は、以下の発明の詳細な説明及び添付図面を参照することによって明らかになる。

【００１７】

【発明の実施の形態】図１は、本発明がネットワークにおいて実装される場合の様式で配置されたデータネット

ワークのコンポーネントを示す模式図である。図１に示された実施例においては、モニタリングノード１３０が、ネットワークリンク１３２内に、ネットワークリンク１３２を介して伝達されるネットワークトラフィックをモニタするように配置されている。モニタリングノード１３０は、モニタされたネットワークトラフィックを特定のユーザに対して実質的にリアルタイムで関連付ける。この、ネットワークトラフィックの特定のユーザに対する関連付けは、モニタリングノード１３０内にストアされた認証データを参照することによって実行される。

【００１８】認証データは、ネットワーク認証ソースからモニタリングノード１３０によって受信される。四つの認証ソース例１１０、１１２、１１４、１１６が図１に示されている。認証ソース１１０、１１２、及び１１４は、データネットワークへのアクセスあるいはデータネットワーク上のアクセス可能な資源へのアクセスを得ることを望むユーザを認証する目的で用いられる。ＮＴドメインサーバは、マイクロソフトＷｉｎｄｏｗｓＮＴのローカルエリアネットワーク上にログオンしているユーザを認証する。ダイアルアップサーバ１１２は、ダイアルアップサービスプロバイダにログインするユーザを認証する。ダイアルアップサーバ１１２は、前述されているように、ＲＡＤＩＵＳサーバを含むことも可能である。共用システム１１４は、例えば、複数のユーザが同時にログオンすることが可能な共用ＵＮＩＸ（登録商標）システムなどの共用コンピュータシステムを表わしている。これらのシステムは、通常、ユーザがユーザＩＤ及びパスワードの入力を行なうことを要求することによってユーザを認証する。認証データをモニタリングノード１３０に供給する目的で、認証ソース１１０、１１２、１１４は、さらに、それぞれモニタ１２０、１２２、１２４を有している。これらのモニタは、ユーザの認証に際して認証データをモニタリングノード１３０宛に送出する追加された機能を実現するソフトウエアモジュールを表わしている。

【００１９】認証サーバ１１０及び１１２に関して、認証データはモニタリングノード１３０宛に、認証サーバ１１０あるいは１１２にいずれかによるユーザの認証に即時に応答して供給される。よって、ユーザの認証がなされると、当該ユーザに係る認証データがモニタリングノード１３０宛に即時に送出される。もちろん、認証サーバ１１０、１１２、モニタ１２０、１２２、及びモニタリングノード１３０との間の通信リンクの設計に起因する通常の処理及び伝播遅延に依る、モニタリングノード１３０による情報受信の遅延は存在することに留意されたい。しかしながら、そのような遅延は副次的なものであり、認証データは、ユーザの認証に引き続いて即時的にモニタリングノード宛に送出されて受信されることが企図されている。共用システム１１４に関しては、認証データはモニタ１２４によって、ユーザによるデータ転送の開始に即時に応答して、モニタリングノード１３０宛に送出される。共用システム１１４及びモニタ１２０、１２２、１２４の詳細に係る側面については、後に詳細に記述される。

【００２０】設置されている認証ノード１１６は、データネットワークへのアクセスを指向するユーザを認証しないが、その代わりに、モニタリングノード１３０に対するアクセスを有する管理機能を代表している。設置されている認証ノード１１６は、モニタリングノード１３０宛の認証データの直接供給を可能にする。後の記述より明らかになるように、認証データの直接供給は、例えば一群のユーザに係る認証データの提供の際などに有用である。

【００２１】モニタリングノード１３０は、ネットワークトラフィックを特定のユーザに関連付ける際、その情報をデータベース１４０宛に供給する。データベース１４０は、情報をストアし、これらのデータをさらに相関付ける目的で、ある種のデータ処理を実行する。その後、データベース１４０は、データをネットワークアプリケーションに対して供給する。あるいは、モニタリングノード１３０は、ネットワークアプリケーションに対して直接データを供給する。ネットワークアプリケーション例は後に詳細に記述される。

【００２２】モニタリングノード１３０の機能ブロック図が図２に示されている。モニタリングノード１３０は、二つのネットワークインターフェース２０２、２０６を有している。ネットワークインターフェースの個々のタイプは、モニタされるネットワークのタイプ（例えば、イーサネット（登録商標））に依存する。ネットワークインターフェースはネットワークドライバ２０４に接続されている。データパケットがいずれかのネットワークインターフェース２０２、２０６において受信されると、ネットワークドライバ２０４は、そのデータパケットをどのように取り扱うかを決定する。データパケットは、以下の三つの一般的なカテゴリに分類されうる。第一に、データパケットは、モニタリングノード１３０以外のネットワークノード宛のデータパケットである可能性がある。この場合には、ネットワークドライバ２０４はそのデータパケットを宛先アドレス宛に伝達する目的で他方のネットワークインターフェースに転送する。ネットワークドライバ２０４は、特定のユーザ及びサービスをデータパケットと関連付ける目的でモニタリングデータ２１４をアクセスする。より詳細に述べれば、ネットワークドライバ２０４は、特定のユーザ及びサービスをデータパケットと関連付ける目的で、認証データ２１８及びサービステーブル２２０をアクセスする。それが成功すると、ネットワークドライバ２０４は利用状況データ２１６を適切に更新する。特定のユーザ及びサービスのデータパケットとの関連付け及び利用状況データ

２１６の更新に関しては、後に詳細に議論される。データパケットの第二のカテゴリは、モニタリング機能の実行に用いられる目的でのモニタリングノード１３０宛のデータパケットである。前述されているように、認証ソース１１０、１１２、１１４、１１６（図１）は、認証データをモニタリングノード１３０宛に送出する。この認証データは、ネットワークを介して送出され、ネットワークノード１３０によって、ネットワークインターフェース２０２、２０６のうちのいずれかにおいて受信される。ネットワークドライバ２０４は、認証ソースからの認証データの受信を認識し、認証データ２１８を適切に更新する。

【００２３】モニタリングノード１３０は、ネットワークトラフィックモニタリングアプリケーション以外の他のネットワークアプリケーションに対するホストとして機能しうることに留意されたい。そのような実施例においては、第三のカテゴリに属するデータパケットが存在し、それらは、モニタリングノード１３０宛ではあるが、そのような他のネットワークアプリケーションに係るものである。ネットワークドライバ２０４はこれらのデータパケットを認識し、それらを処理目的でＩＰプロトコルスタック２０８宛に転送する。

【００２４】ネットワークノード１３０は、モニタリングノード１３０のモニタリング機能のうちのいくつかを制御するコントローラ２２２も含んでいる。コントローラ２２２は、他のネットワークエレメントとの通信を可能にするＩＰプロトコルスタック２０８との通信を行なう。コントローラ２２２の機能の一つは、サービステーブル２２０と、他の認証ノード２１６などの外部ネットワークノードから得られた認証データ２１８の管理を制御することである。コントローラ２２２は、さらに、モニタリングノード１３０からデータベース１４０への利用状況データ２１６の転送をも制御する。ここで示されている実施例においては、コントローラ２２２は、ＩＰプロトコルスタック２０８を介しネットワークインターフェース２０２、２０６のうちのいずれかを通じてデータベース１４０と通信する。別の実施例においては、コントローラ２２２は、専用（図示せず）のＩ／Ｏポートを介してデータベース１４０と通信する。

【００２５】モニタリングノード１３０は、適切にコンフィギュアされてプログラミングされたデジタルコンピュータを用いて実装されうる。よって、本明細書において記述されるモニタリングノードの機能は、ストアされたコンピュータプログラムコードを実行するプロセッサの制御下で実行される。プログラムされたデジタルコンピュータは当業者には公知であり、プログラムされたデジタルコンピュータを用いてモニタリングノード１３０を実装するために必要となるプロセッサ、メモリなどの公知のコンポーネントは図２には示されていない。当業者は、本明細書における記述が与えられれば、モニタリングノードを容易に実装することが可能である。ネットワークインターフェース２０２、２０６は、コンピュータの一部でありうるハードウエアデバイスを表わしている。ネットワークドライバ２０４、ＩＰプロトコルスタック２０８、及びコントローラ２２２は、本明細書に記載されている機能を実装するために用いられるソフトウエアモジュールを表わしている。

【００２６】図２に示されているように、ＩＰプロトコルスタック２０８、ネットワークドライバ２０４、及びモニタリングデータ２１４は、コンピュータのオペレーティングシステムカーネル空間２２６内のメモリに配置されている。カーネル空間２２６は、オペレーティングシステムカーネルによってのみアクセス可能な部分のコンピュータメモリを表わしている。コントローラ２２２は、ユーザ空間２２４内に位置している。ユーザ空間２２４は、ユーザソフトウエアモジュールによってアクセス可能な部分のコンピュータメモリを表わしている。一般に、カーネル空間２２６内でなされる処理は、ユーザ空間２２４内でなされる処理よりも高速である。図２に示されたアーキテクチャは、大部分のデータパケット処理プロセスがカーネル空間２２６内でなされるために有利である。さらに、このアーキテクチャは、データパケットをカーネル空間２２６からユーザ空間に移動するという付加的なコストを回避している。コントローラ２２２は、その処理時間が重要になるような操作を行なわないために、ユーザ空間２２４に適切に配置されている。このような本発明に係るモニタリングノード機能の有利な設計により、受信したデータパケットの特定のユーザへの関連付けが実質的にリアルタイムでサポートされる。別の実施例においては、データパケット処理機能のうちのある部分あるいはその全てがユーザ空間２２４において実行される。このことによって付加的なオーバーヘッドが導入されるが、ソフトウエア開発及び管理が簡潔化される。

【００２７】モニタリングデータ２１４は、図３から図５を参照してより詳細に記述される。図３は、ストアされた利用状況データ２１６のフォーマットを示しており、それは、モニタリングノード１３０によってその動作の間に収集されたモニタリング情報を含んでいる。利用状況データ２１６は、図３に示された形式の記録を含んでいる。ユーザフィールド３０２はデータパケットに関連付けられた特定のユーザを識別し、ｓｒｖｃフィールド３０４は特定のユーザによって用いられるサービスを識別する。これらの記録における残りの部分のデータは、ユーザフィールド３０２及びサービスフィールド３０４に基づいて集積されたものである。よって、特定のサービスを用いる特定のユーザに関しては、単一の記録が存在して、残りのフィールドはモニタリングが継続されるに連れて集積される。バイト数フィールド３０６は転送されたバイト数を含んでいる。パケット数フィール

ド３０８は転送されたパケット数を含んでいる。フロー数フィールド３１０はフロー数を含んでいる。ｓｒｃ－ＩＰフィールド３１２はデータパケットのソースＩＰアドレスを含んでいる。ｄｓｔ－ＩＰフィールド３１４はデータパケットのデスティネーションＩＰアドレスを含んでいる。ｓｒｃ－ｐｒｔフィールド３１６はデータパケットのソースポートを含んでいる。ｄｓｔ－ｐｒｔフィールド３１８はデータパケットのデスティネーションアドレスを含んでいる。後ろ側の四つのフィールド３１２、３１４、３１６、３１８はオプションであり、相異なったユーザ、サービス、あるいはホストに関して管理される場合もあり、管理されない場合もある。これらのフィールドが管理されない場合には、性能が向上する。しかしながら、例えば、特定のユーザによる利用状況を詳しく監査する目的などのように、より詳細な情報を管理することが望ましい場合も存在する。

【００２８】多くのコンピューティング環境においては、複数個の認証ドメインが共存している。例えば、単一のローカルエリアネットワークは、ＮＴドメイン認証及びＵＮＩＸドメイン認証の双方をサポートしうる。さらに、ダイアルアップ接続に関しては、リモートアクセス認証が用いられうる。このことによって、単一のユーザが複数のドメインに亘って複数個のユーザ名を有しうるという問題が生ずる。従って、同一のユーザ名が複数の認証ドメインにおいて、相異なったユーザに対して割り当てられる可能性がある。この問題を処理する目的で、利用状況データ記録のユーザフィールド３０２は、さらに三つのフィールドに分割される。ドメインフィールド３２０は認証ドメインを識別する。認証ドメインが明示的に知られていない場合、ドメイン名を割り当てる一つの技法は、認証を実行しているシステムのＩＰアドレス（例えば、ＮＴドメインサーバのＩＰアドレス）あるいは認証を実行している機械に係るプロキシのＩＰアドレスを用いることである。タイプフィールド３２２は実行された認証のタイプである。例えば、このタイプは、認証サーバのタイプに依存して、“ＵＮＩＸ”、“ＮＴ”、あるいは“ＲＡＤＩＵＳ”として識別される。ｕｉｄフィールド３２４は、その特定のドメインに係るユーザ識別子である。ドメインフィールド３２０、タイプフィールド３２２、及びｕｉｄフィールド３２４をユーザ識別目的で利用することにより、利用状況データの監査も可能になる。この種の監査には、モニタが利用状況を特定のユーザに関してどのように関連付けたかに係る事後の決定が含まれる。

【００２９】ネットワーク利用状況を特定のユーザに関連付けるのみならず、モニタリングノード１３０は、ユーザによって利用されているサービスを識別する機能をも有している。ｓｒｖｃフィールド３０４は、さらに三つのフィールドに分割されている。サービスタイプフィールド３２６はサービスタイプを識別する。本発明の一実施例においては、サービスタイプフィールド３２６は、ＥＴＨＥＲ、ＩＰ、ＴＣＰ、あるいはＵＤＰを含む。ＩＰアドレスフィールド３２８はＩＰアドレスを含んでいる。サービスフィールド３３０は、サービスタイプフィールド３２６によって規定されたサービスクラス内の特定のサービスを識別するコンテクストセンシティブコードを含んでいる。本発明の一実施例において、サービスタイプフィールド３２６がＥＴＨＥＲである場合には、サービスフィールド３３０はイーサネットプロトコル番号を有している。サービスタイプフィールド３２６がＩＰである場合には、サービスフィールド３３０は標準的なＩＰプロトコル番号（例えば、ＩＰ／ＩＣＭＰに関しては１、ＩＰ／ＴＣＰに関しては６、及び、ＩＰ／ＵＤＰに関しては１７）を有している。サービスタイプフィールド３２６がＴＣＰあるいはＵＤＰの場合には、サービスフィールド３３０はサービスのポート番号（ＨＴＴＰの場合には、サービスタイプフィールド３２６はＴＣＰを有しており、サービスフィールド３３０は８０を有している；これは、ＨＴＴＰサービスに関する標準的なポートである）を有している。

【００３０】図４は、ストアされた認証データ２１８記録のフォーマットを示している。これらの記録におけるデータは、認証ソースから受信され、モニタされたネットワークトラフィックを特定のユーザに関連付ける目的で利用される。認証データ２１８は、特定のユーザにＩＰアドレス、プロトコル、及びポートを関連付ける記録を有している。それらのフィールドに関しては以下に概説されるが、これらのフィールドの、特定のユーザに対してネットワークトラフィックを関連付ける目的での利用に関しては、後に詳述される。ＩＰ－ａｄｄｒフィールド４０２はＩＰアドレスを有しており、マスクフィールド４０４はマスクとして用いられる３２ビット数を有しており、ｐｒｏｔｏフィールド４０６はＩＰプロトコル番号（例えば、ＵＤＰ（１７）あるいはＴＣＰ（６））を有しており、ポートフィールド４０８はポートの識別を有しており、及びユーザフィールド４１０は特定のユーザを識別する。ユーザフィールド４１０は、さらに、ドメインフィールド４１２、タイプフィールド４１４、及びｕｉｄフィールド４１６に分割されている。フィールド４１２、４１４、及び４１６は、図３に関連して上述されているフィールド３２０、３２２、及び３２４と同一である。

【００３１】図５は、サービステーブル２２０の記録のフォーマットを示している。これは、特定のユーザの利用状況に関連付けられたサービスを識別する目的で用いられる。そのフィールドに関しては以下に概説されるが、ネットワークトラフィックを特定のユーザに関して関連付ける目的でのこれらのフィールドの利用に関しては後に詳述され、その時点でこれらのフィールドの利用が明確になる。ＩＰ－ａｄｄｒフィールド５０２、マス

クフィールド５０４、及びｐｒｏｔｏフィールド５０６は、図４に関連して上述されたフィールド４０２、４０４、及び４０６と同一である。ポート範囲フィールド５０８はポート識別の範囲を有している。

【００３２】図６は、ＩＰプロトコルに従ったＴＣＰデータパケットのフォーマットを示している。ＩＰプロトコルは公知であり、本発明に関連しているフィールドのみが記述される。データパケット６００は、ＩＰヘッダ６０２、ＴＣＰヘッダ６０４及びＴＣＰデータ６０６を含んでいる。ＩＰヘッダ６０２は、プロトコル６０８、ソースＩＰアドレス６１０及びデスティネーションＩＰアドレス６１２を含む複数のフィールドより構成されている。ＴＣＰヘッダ６０４も、ソースポート６１４及びデスティネーションポート６１６を含む複数個のフィールドより構成されている。図６に示されたＴＣＰデータパケットは、本発明に従って処理されるデータパケットの一例である。しかしながら、本発明はＴＣＰパケットの処理に限定されているわけではない。当業者には、本発明が他のプロトコルに従って送信されるデータパケットの処理を行ないうることが明白である。例えば、それらのプロトコルにはイーサネット、ＩＰ、ＵＤＰ、ＲＰＣ、ＮＦＳ（登録商標）、ＳＭＰＴなどがあるが、それらに限定されている訳ではない。

【００３３】本発明に従ったモニタリングノード１３０の動作が図７から図９の流れ図を参照して以下に記述される。流れ図に示された段階は、ストアされたコンピュータプログラムコードに従って、モニタリングノード１３０のプロセッサによって実行される。図７は、データパケットを受信した際にモニタリングノード１３０によって実行される段階を示している。段階７０２では、データパケットがモニタリングノード１３０によって受信される。このパケットは、モニタリングノード１３０以外のネットワークノードに宛てたものであって、モニタリングノード１３０がそのデータパケットへの特定のユーザ及びサービスの関連づけを試行している、ということが仮定されている。段階７０４では、モニタリングノード１３０は、受信したデータパケットが、特別の処理が必要とされるある種の既知のプロトコルに従ってデータを伝達しているデータパケットであるか否かを決定する。データパケットの特別な処理に関しては後述される。データパケットが特別の処理を必要とするデータを伝達していない場合には、制御が段階７０６へ進み、そのデータパケットのソースであるユーザの識別に係る試行がなされる。ユーザ識別段階７０６は、さらに、図８に示された流れ図に関連して詳述される段階も含んでいる。ユーザが識別されない場合には、段階７１０において、データパケットの宛先であるユーザの識別に係る試行がなされる。この段階７１０は段階７０６と同一であり、後に図８に関連して詳述される。段階７１２においては、段階７１０でユーザが識別されたか否かが決定される。ユーザが段階７０８あるいは段階７１２において識別された場合には、段階７１４において、データパケットに関連付けられたサービスの識別が試行される。段階７１２においてユーザが識別されなかった場合には、この方法は段階７１８で終了する。サービス識別段階７１４は、後に図９の流れ図に関連して詳述される段階を含んでいる。段階７１６においては、利用状況データ２１６（図２）が段階７０６あるいは７１０において識別されたユーザ、及びサービス（段階７１４で識別された場合）に従って更新される。

【００３４】段階７０４では、受信されたパケットが特別の処理を必要とするか否かが決定される。ある種のプロトコルは、データを、当該データを送出するユーザが当該データを送出するように要求されたユーザではない、という様式で送出する。例えば、ＵＮＩＸシステム上のネットワークファイルシステム（ＮＦＳ）プロトコル要求は、通常、システム管理者によって所有されるプロセスによって開始され、データを要求しているユーザによって所有されるプロセスからではない。同様に、ｅメール（電子メール）も、メールを送信するユーザによってではなく、メーラーデーモンによって所有されるプロセスによってフォワードされる。別の例は、ウェブ（ｗｅｂ）ホストサービスを提供するウェブサーバである。ウェブサーバはデータを伝送するが、考慮されるべきユーザはその内容が転送される宛先のユーザである。これら、また他の特別な場合において、アプリケーションに特有の技法が、ネットワークを介したデータの発信あるいは受信を行なっているユーザを識別する目的で用いられなければならない。最も一般的には、これらの技法には、パケットヘッダのみならずそのパケットの内容に対する調査が含まれる。よって、段階７０４におけるテストがｙｅｓである場合には、段階７２０において、特別の処理アルゴリズムがユーザ識別を決定する目的でデータパケットに対して適用される。標準的ではないプロトコルの各々は、それぞれに係る特別の処理アルゴリズムを有している。データ通信の当業者は、所定のプロトコルに対するその種のアルゴリズムを容易に実装可能である。

【００３５】図３を参照して、利用状況データ２１６における記録は、新たなユーザ識別及びサービス識別を（それぞれ存在する場合には）反映するように更新される。識別されたユーザ及びサービス対を含む利用状況記録が既に存在する場合には、バイト数フィールド３０６、パケット数フィールド３０８及びフロー数フィールド３１０が、その新たなデータパケットを反映するように更新される。識別されたユーザ及びサービス対を含む利用状況データ記録が存在していない場合には、適切な情報を含む新たな記録が生成される。このようにしてユーザデータ２１６を更新することにより、それぞれ独自のユーザ／サービス対の各々に対して単一の記録が生成

される。

【００３６】図８は、特定のデータパケットに係るユーザを識別する段階７０６、７１０をより詳細に示した流れ図である。段階７０６の結果として図８に示された段階が実行される場合は、ＩＰアドレスは受信されたデータパケットのソースＩＰアドレス６１０（図６）である。段階７１０の結果として図８に示された段階が実行される場合は、ＩＰアドレスは受信されたデータパケットのデスティネーションＩＰアドレス６１２である。段階８０２では、認証データ記録２１８に対する指数（ｉ）が１にセットされる。図８における記述で用いられる“フィールド名”［ｉ］という表現は、認証データ２１８におけるｉ番目の記録における“フィールド名”を有するフィールドの値を表わしている。段階８０４では、データパケットのＩＰアドレスにマスク［ｉ］が適用される。二つの値を比較する前にマスクを適用することは公知の技法である。ここでは、マスクが、データパケットのＩＰアドレスの範囲が単一の認証データ記録のＩＰ－ａｄｄｒ（フィールド４０２）に一致するか否かを検出する目的で用いられる。このことは、例えば、特定のサブネットに属するユーザを識別するような課金アプリケーションにおいて有用である。

【００３７】段階８０６では、マスクされたデータパケットのＩＰアドレスがＩＰ－ａｄｄｒ［ｉ］と比較される。一致がない場合には、段階８０８において、認証データ２１８内に別の記録が存在するか否かが決定される。別の記録が存在しない場合には一致はなく、この方法は段階８３０で終了する。さらなる記録が存在する場合には、段階８１０において指数ｉが１だけ増加させられ、制御は８０４へ戻る。マスクされたデータパケットのＩＰアドレスがＩＰ－ａｄｄｒ［ｉ］と一致する場合には、段階８０６でのテストの結果はＹＥＳであって、段階８１２において、ｐｒｏｔｏ［ｉ］が規定されているか否かが決定される。すなわち、段階８１２は、ｉ番目の認証記録におけるｐｒｏｔｏフィールド４０６が値を有しているか否かを決定する。有していない場合には一致はなく、この方法は段階８３０で終了する。段階８１２のテスト結果がＹＥＳである場合には、段階８１４で、受信されたデータパケットのプロトコル（フィールド６０８）がｐｒｏｔｏ［ｉ］と一致するか否かが決定される。段階８１４のテスト結果がＮＯである場合には、ｉ番目の認証記録は受信されたデータパケットと一致せず、制御は段階８０８へ移る。段階８１４のテスト結果がＹＥＳである場合には、段階８１６において、ｐｒｏｔｏ［ｉ］がＴＣＰあるいはＵＤＰであるか否かが決定される。段階８１６のテスト結果がＮＯである場合には、一致が存在し、この方法は段階８３０で終了する。段階８１６でのテスト結果がＹＥＳである場合には、段階８１８において、ｐｏｒｔ［ｉ］が規定されているか否かが決定される。規定されていない場合には、一致が存在し、この方法は段階８３０で終了する。段階８１８でのテスト結果がＹＥＳである場合には、段階８２０において、受信されたデータパケットのポート（図８に示された方法が図７の段階７０６から実行された場合にはソースポートフィールド６１４であり、図８に示された方法が図７の段階７１０から実行された場合にはデスティネーションポートフィールド６１６である）がｐｏｒｔ［ｉ］と一致するか否かが調べられる。段階８２０のテスト結果がＮＯである場合には、ｉ番目の認証記録は受信されたデータパケットと一致せず、処理は段階８０８へ戻る。段階８２０のテスト結果がＹＥＳである場合には、一致が存在し、この方法は段階８３０で終了する。

【００３８】図９は、特定のデータパケットに係るサービスを識別する段階７１４（図７）をより詳細に示した流れ図である。図９に示された段階は、まず、受信されたデータパケットをサービスに関連付ける目的で、受信されたデータパケット６００のソースＩＰアドレスフィールド６１０及びソースポートフィールド６１４を用いることによって実行される。ソースＩＰアドレスフィールド６１０及びソースポートフィールド６１４を用いてサービスが見出さない場合には、図９の段階は、受信されたデータパケットをサービスに関連付ける目的で、受信されたデータパケット６００のデスティネーションＩＰアドレスフィールド６１２及びデスティネーションポートフィールド６１６を用いることによって実行される。

【００３９】段階９０２では、サービステーブル２２０に係る指数（ｉ）が１にセットされる。図９の記述に関しては、フィールド名［ｉ］という表現は、サービステーブル２２０におけるｉ番目の記録のフィールド名を有するフィールドの値を示している。段階９０４においては、データパケットのＩＰアドレスがマスク［ｉ］によってマスクされる。段階９０６では、マスクされたデータパケットのＩＰアドレスが、ＩＰ－ａｄｄｒ［ｉ］と比較される。一致がない場合には、段階９０８において、サービステーブル２２０にさらに記録が存在しているか否かが決定される。記録が存在しない場合には、そのサービスは未知であってこの方法は段階９２２で終了する。さらに記録が存在する場合には、段階９１０において指数ｉが１だけ増加させられて、制御が段階９０４に戻る。マスクされたデータパケットのＩＰアドレスがＩＰ－ａｄｄｒ［ｉ］と一致する場合には、段階９０６でのテスト結果がＹＥＳであり、段階９１１においてｐｒｏｔｏ［ｉ］が規定されているか否かが決定される。すなわち、段階９１１は、ｉ番目のサービステーブル記録におけるｐｒｏｔｏフィールドが値を有しているか否かを決定する。値を有していない場合には、一致が存在して制御は段階９１６へ進む。段階９１１のテスト結果がＹＥＳである場合には、段階９１２において、受信さ

れたデータパケットのプロトコル（フィールド６０８）がｐｒｏｔｏ［ｉ］と一致するか否かが決定される。段階９１２におけるテスト結果がＮＯである場合には、ｉ番目のサービステーブル記録は受信されたデータパケットと一致せず、制御は段階９０８へ進む。段階９１２におけるテスト結果がＹＥＳである場合には、段階９１３において、ｐｏｒｔ－ｒａｎｇｅ［ｉ］が規定されているか否かが決定される。すなわち、段階９１３は、ｉ番目のサービステーブル記録におけるポート範囲フィールド５０８が値を有しているか否かを決定する。値を有していない場合には、一致が存在して制御は段階９１６へ進む。段階９１３におけるテスト結果がＹＥＳである場合には、段階９１４において、受信されたデータパケットのポートがｐｏｒｔ－ｒａｎｇｅ［ｉ］によって規定された範囲内にあるか否かが決定される。段階９１４のテスト結果がＮＯである場合には、ｉ番目のサービステーブル記録は受信されたデータパケットと一致せず、制御は段階９０８へ進む。段階９１４におけるテスト結果がＹＥＳである場合には、段階９１６に示されているようにサービスが識別されたことになる。よって、利用状況データ２１６が段階７１６において更新される際には、サービスタイプフィールド３２６には受信されたデータパケットのプロトコル（フィールド６０８）の値が割り当てられ、ＩＰ－ａｄｄｒフィールド３２８にはマスクされたデータパケットのＩＰアドレス（段階９０４で決定されたもの）が割り当てられ、サービスフィールド３３０にはデータパケットのポートの値が割り当てられる。この方法は段階９２２で終了する。

【００４０】以下、モニタ１２０、１２２、及び１２４の実装の詳細な議論が記述される。

【００４１】ある実施例においては、モニタ１２０及び１２２は、それぞれ認証サーバ１１０及び１１２の認証ログをモニタする。認証ログに対して新たな認証データが生成されると、関連しているモニタがその情報をモニタリングノード１３０宛に即時転送する。

【００４２】ＮＴドメインサーバ１１０に係るモニタ１２０の別の実施例においては、モニタ１２０は、ネットワーククリティカルオペレーション（例えば、ログオン及びログオフなど）の性能に係る通知を自動的に受信するように登録されたＮＴサービスとして実装される。この種の通知を受信すると、モニタ１２０は適切な認証データをモニタリングノード１３０宛に即時送信する。

【００４３】ダイアルアップサーバ１１２に関しては、ある種のダイアルアップサーバはＮＴドメインサーバ１１０に関連して上述されているものと同様の通知機構を実現し、これらは認証モニタ１２２を実装する目的で用いられる。加えて、ダイアルアップサーバ１１２がＲＡＤＩＵＳサーバとして実装される場合には、モニタ１２２はＲＡＤＩＵＳクライアントと実際のＲＡＤＩＵＳサーバとの間のプロキシＲＡＤＩＵＳサーバとして実装されうる。この実装においては、プロキシはクライアントとＲＡＤＩＵＳサーバとの間の全ＲＡＤＩＵＳ要求及び応答を転送する。加えて、副次的な効果として、プロキシはユーザ認証に即時に応答してモニタリングノード１３０宛に認証データを生成して送出する。

【００４４】以下、共用コンピュータシステム１１４に係るモニタ１２４の一つの有利な実施例が記述される。この実施例においては、ＵＮＩＸオペレーティングシステムの共有オブジェクトアーキテクチャ及び動的リンキング機能が用いられている。共有ライブラリは、ワールドワイドウェブサーバ及びブラウザ、及びＦＴＰサーバ及びクライアントなどの標準的なネットワークアプリケーションに対して、オペレーティングシステムによって自動的に動的にリンクされる。この実施例に従って、既存の共有ソケットライブラリ（通常、libsocket.soと呼称されるもの）が、新たなソケットライブラリによって置換される。この新たなライブラリは、元のソケットライブラリと同一のオペレーションの全てを含んでおり、さらに、ネットワークオペレーションの少なくともいくつかに関して、付加的なラッパーコードが挿入されている。この有利な実施例において、新たなコードでラップされている機能には、ｂｉｎｄ、ｃｏｎｎｅｃｔ、ｓｅｎｄｍｓｇ、ｓｅｎｄｔｏ、ｒｅｃｖｆｒｏｍ、及びｒｅｃｖｍｓｇが含まれる。これらの機能が実行される際には、付加されたラッパーコードは、認証データをモニタリングノード１３０宛に送出する認証メッセージを生成する。認証情報は、通常、共有コンピュータシステム１１４のＩＰアドレス、特定のユーザのプロセスが通信しているＴＣＰ及びＵＤＰポート、及び当該ユーザの識別を含んでいる。よって、この状況では、認証データは、ユーザによるデータ転送の開始に即時に応答して送出される。

【００４５】モニタ１２０、１２２、１２４に係る上記記述は、モニタがどのようにして認証データを生成するかに係るものである。ひとたび生成されると、認証データはモニタリングノード１３０宛に送出される。図１においては、モニタリングノード１３０が認証ソース１１０、１１２、１１４、１１６に接続されているように示されているが、これは論理的な接続であって、実際、認証ソース１１０、１１２、１１４、１１６からモニタリングノード１３０宛に送出される認証データは、単一あるいは複数個のサブネットワークを通過することを求められる場合があることに留意されたい。加えて、認証データは、データネットワークの複数個のサブネットワークにおける複数個のモニタリングノード宛に送出される場合もある。以下、認証データをモニタリングノード宛に送出するための二つの方法が記述される。

【００４６】認証サーバ１１０及び１１２は、ブロードキャスト認証と呼称される方法を用いており、認証データは認証サーバからモニタリングノード宛の特別なメッ

セージにおける認証データとして送出される。これらのメッセージは、モニタリングノードが位置しているサブネットワークにおけるブロードキャストアドレス宛に送出される。これらの特別のメッセージは、モニタリングノードによって受信されて処理される。モニタリングノードが位置しているサブネットワークのブロードキャストアドレスは、認証サーバ１１０、１１２に与えられている。

【００４７】共有コンピュータシステムよりなる認証ソース１１４は、認証データをモニタリングノード宛に送出するための二つの技法のうちの一方を用いる。前述されているように、共用コンピュータシステム１１４のモニタ１２４は、共用システム１１４のユーザによるデータ転送の開始に際して認証データを送出する。ユーザが接続指向送信を開始する際には、前述されたブロードキャスト認証技法が用いられる。認証ソース１１４によってブロードキャスト認証が用いられる場合には、ブロードキャストアドレスはその機械が接続されているサブネットワークのブロードキャストアドレスである。そのサブネットワーク宛に送出することによって、全ての介在するモニタリングノードが認証データを含む特別のメッセージを受信することが可能になる。ユーザが接続無し送信を開始する場合には、共有システム１１４は、タグ認証と呼称される別の方法を利用する。この方法に従って、全ての発信メッセージには付加的な認証データがタグとして付加される。発信メッセージにタグを付加する一つの方法は、認証データをＩＰパケットヘッダのオプションフィールドに挿入することである。この技法は、発信メッセージにのみ作用する（なぜなら、着信メッセージにはタグが付されえないからである）。接続無し送信における発信メッセージに関しては、前述されたブロードキャスト認証も用いられうることに留意されたい。タグあるいはブロードキャスト認証のいずれを発信データパケットに対して用いるかは、送出されるパケットの予想数に依存する。接続無し送信における着信パケットに関しては、ブロードキャスト認証が用いられなければならない。しかしながら、モニタリングノードは、データパケットを正確に処理することが可能であるためには、データパケットの受信前に認証データのブロードキャストを受信しなければならない。このタイミング問題を取り扱う一つの技法は、モニタリングノードがブロードキャスト認証データを受信するまで、接続無し送信における入力パケットをバッファリングすることである。

【００４８】データパケットに係るユーザ及びサービス情報を決定するための上述された方法は、完全なＩＰ及び関連している場合にはＴＣＰあるいはＵＤＰヘッダが利用可能である場合に用いられる。しかしながら、ある種のネットワークにおいては、大きなメッセージが複数個のより小さいパケットに分断されてしまう。上述されているような、ユーザ及びサービスを決定するために必要とされるヘッダ情報は、分断されたパケットのうちの最初のもののみにおいて利用可能である。このような状況を取り扱う目的で、第一パケットから決定されたユーザ及びサービス情報は、モニタリングノード１３０内にストアされうる。同一メッセージの残りの部分がモニタリングノード１３０において受信された際に、ストアされたユーザ及びサービス情報がその残りの部分に対しても適用される。ＩＰヘッダにストアされた分断情報は、モニタリングノード１３０が分断されたパケットをそれ以前に受信されたヘッダから適切なユーザ及びサービス情報に関連付けることを可能にする。

【００４９】以上の記述より明らかなように、モニタリングノード１３０は、特定のユーザのネットワークトラフィックに対する関連づけを可能にする。この技法と共に用いられうるネットワークアプリケーションは多数存在する。課金アプリケーションは、ネットワークトラフィック量、日時、及び用いられた特定のサービス等のファクタを含む、特定のユーザによるネットワーク利用状況に基づいて特定のユーザに課金する目的で、データベース１４０にストアされたネットワーク利用状況を利用できる。サービス品質（ＱｏＳ）ネットワークアプリケーションも実装可能である。モニタリングノード１３０を用いることにより、特定のユーザによって受容されるサービス品質をモニタすることが可能になる。ＱｏＳネットワークアプリケーションは、ＱｏＳサービスが所定のレベル未満に低下した場合にユーザに弁済する目的で用いられることも可能であり、また、ＱｏＳの所定のレベルを回復するためにネットワークにおける修正操作を行なう目的ででも用いられうる。例えば、ＩＰテレフォニーの双端における二つのモニタリングノードが、通話によって受容されるエンドーツーエンドサービス品質を測定する目的で使用されうる。これは、例えば平均あるいは最大レイテンシの観点で測定される。この情報は、種々の料金プランの基礎を構成しうる。ファイアウォールアプリケーションは、特定のソースあるいはデスティネーションユーザに基づくネットワークトラフィックを制限する目的で用いられる。現時点のファイアウォールは、通常、ソースあるいはデスティネーションＩＰアドレスに基づいてトラフィックを制限する。しかしながら、前述されているように、ＩＰアドレスは特定のユーザを識別しない。上述されたネットワークモニタを用いることにより、ファイアウォールアプリケーションが特定のユーザに基づいてネットワークトラフィックを制限することが可能になる。課金アプリケーション、サービス品質アプリケーション、及びファイアウォールアプリケーションは専用のネットワークノードを用いて実装されうる。あるいは、課金アプリケーション、サービス品質アプリケーション、及びファイアウォールアプリケーションが、スイッチやルータなどの他の目的で用いられうるネットワークノードに組み込まれることも可能で

ある。

【００５０】ネットワークトラフィックを特定のユーザに関連付けるデータを用いて他の多くのアプリケーションが実装されうることは当業者には明らかである。例えば、ゲートウェイシステムは、モニタリングノードによって生成された情報を、特定のユーザあるいは特定のユーザクラスから特定のユーザあるいは特定のユーザクラスへのトラフィックを制限する目的で利用することが可能である。ネットワークモニタが特定のユーザによる利用状況をその利用状況が発生する時点で実質的にリアルタイムでモニタするため、プリペイドサービスが実現されうる。さらに、モニタリングノードによって生成されたデータは、時刻、持続時間、あるいは特定のサービス等のファクタに基づいてある種のネットワークポリシーを強要する目的にも用いられうる。

【００５１】ある種のネットワークトポロジーにおいては、複数個のモニタリングノードが存在しうる。結果として、そこをデータパケットが通過するとそれらが複数個のモニタリングノードによって処理されてしまうような経路が存在しうる。このことは、ある種のネットワークアプリケーションに関しては問題となりうる。例えば、課金アプリケーションにおいては、同一のデータパケットを複数個のモニタリングノードにおいて処理することは正しくない。なぜなら、二重課金になってしまうからである。この多重処理の問題及びそれを解決するための技法は、共願されている“データネットワークにおける単一処理の適用のための方法及びその装置”という表題の米国特許出願第09/316118号（1999年5月20日出願）に記載されている。

【００５２】以上の説明は、本発明の一実施例に関するもので，この技術分野の当業者であれば、本発明の種々の変形例が考え得るが、それらはいずれも本発明の技術的範囲に包含される。例えば、図１に示された特定の実施例に関連して記述されているように、モニタリングノード１３０はネットワークリンク上のブリッジとして機能するスタンドアローンネットワークノードとして示されている。しかしながら、本発明に従ったモニタリングノード１３０の機能は、例えばスイッチやルータなどの既存のネットワークノード内のモジュールとして実装されうる。さらに、ある実施例においては、本発明は適切にプログラミングされた汎用コンピュータを用いて実装される。あるいは、本発明は、プログラム可能ハードウェアロジックあるいは専用ハードウェアコンポーネントを用いて実装されることも可能である。

【００５３】

【発明の効果】以上述べたごとく、本発明によれば、ネットワークトラフィックを特定のユーザに対して実質的にリアルタイムで関連付ける方法が提供される。

【図面の簡単な説明】

【図１】　本発明がネットワークにおいて実装される場合の様式で配置されたデータネットワークのコンポーネントを示す図。

【図２】　本発明に係るモニタリングノードの機能を示すブロック図。

【図３】　本発明に係る利用状況データレコードのフォーマットを示す模式図。

【図４】　本発明に係る認証データレコードのフォーマットを示す模式図。

【図５】　本発明に係るサービステーブルレコードのフォーマットを示す模式図。

【図６】　ＩＰプロトコルに従ったＴＣＰデータパケットのフォーマットを示す模式図。

【図７】　本発明に従って、データパケットを受信した際にモニタリングノードによって実行される段階を示す流れ図。

【図８】　本発明に従って、特定のデータパケットに係るユーザを識別する目的でモニタリングノードによって実行される段階を示す流れ図。

【図９】　本発明に従って、特定のデータパケットに係るサービスを識別する目的でモニタリングノードによって実行される段階を示す流れ図。

【符号の説明】

１１０　ＮＴドメインサーバ
１１２　ダイアルアップサーバ
１１４　共有システム
１１６　認証ノード
１２０、１２２、１２４　モニタ
１３０　モニタリングノード
１４０　データベース
２０２　ネットワークインターフェース
２０４　ネットワークドライバ
２０６　ネットワークインターフェース
２０８　ＩＰプロトコルスタック
２１４　モニタリングノード
２１６　利用状況データ
２１８　認証データ
２２０　サービステーブル
２２２　コントローラ
２２４　ユーザ空間
２２６　カーネル空間
３０２　ユーザフィールド
３０４　サービスフィールド
３０６　バイト数フィールド
３０８　パケット数フィールド
３１０　フロー数フィールド
３１２　ソースＩＰアドレスフィールド
３１４　デスティネーションＩＰアドレスフィールド
３１６　ソースポートフィールド
３１８　デスティネーションポートフィールド
３２０　ドメインフィールド

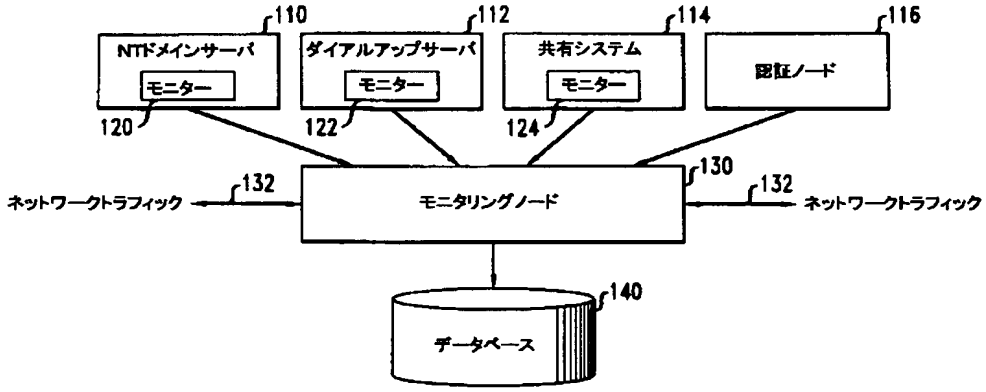
25

３２２　タイプフィールド
３２４　ユーザＩＤフィールド
３２６　サービスタイプフィールド
３２８　ＩＰアドレスフィールド
３３０　サービスフィールド
４０２　ＩＰアドレスフィールド
４０４　マスクフィールド
４０６　プロトコルフィールド
４０８　ポートフィールド
４１０　ユーザフィールド
４１２　ドメインフィールド
４１４　タイプフィールド
４１６　ユーザＩＤフィールド

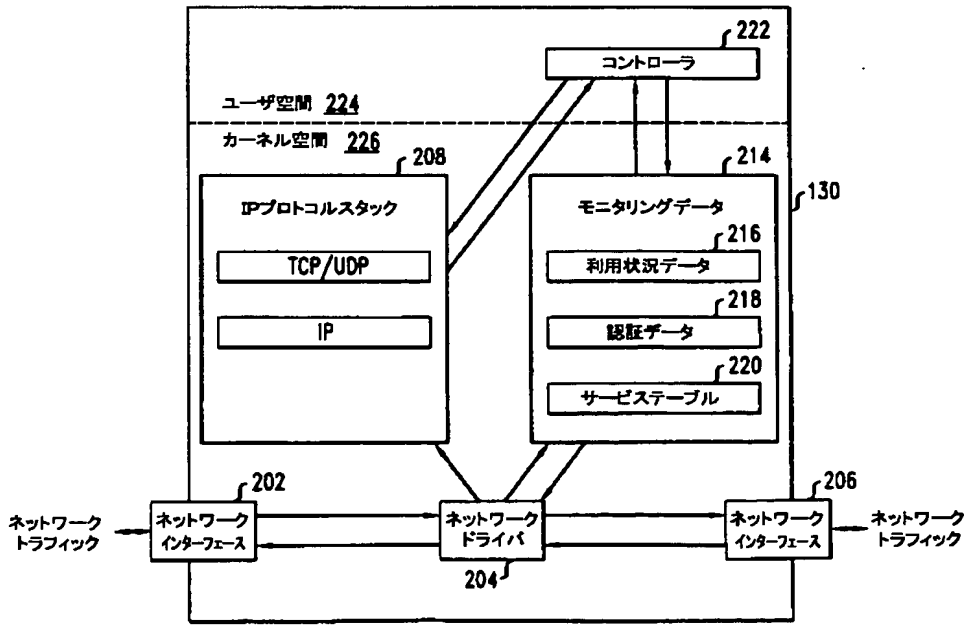
26

５０２　ＩＰアドレスフィールド
５０４　マスクフィールド
５０６　プロトコルフィールド
５０８　ポート範囲フィールド
６００　データパケット
６０２　ＩＰヘッダ
６０４　ＴＣＰヘッダ
６０６　ＴＣＰデータ
６０８　プロトコルフィールド
６１０　ソースＩＰアドレスフィールド
６１２　デスティネーションＩＰアドレスフィールド
６１４　ソースポートフィールド
６１６　デスティネーションポートフィールド

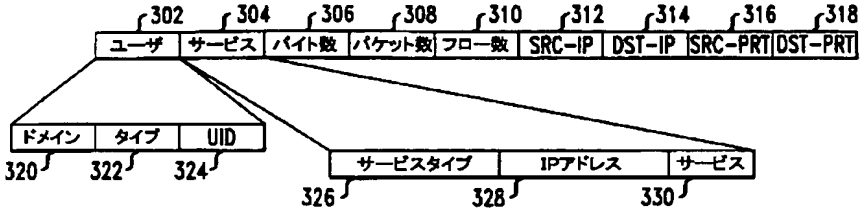
【図１】



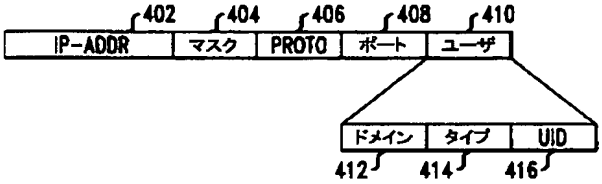
【図２】



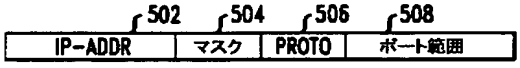
【図３】


302
304
306
308
310
312
314
316
318
ユーザ
サービス
バイト数
パケット数
フロー数
SRC-IP
DST-IP
SRC-PRT
DST-PRT
ドメイン
タイプ
UID
320
322
324
サービスタイプ
IPアドレス
サービス
326
328
330

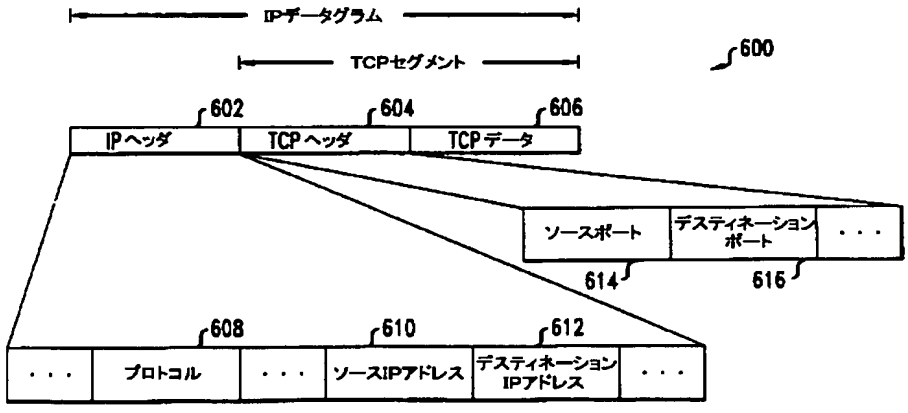
【図４】


402
404
406
408
410
IP-ADDR
マスク
PROTO
ポート
ユーザ
ドメイン
タイプ
UID
412
414
416

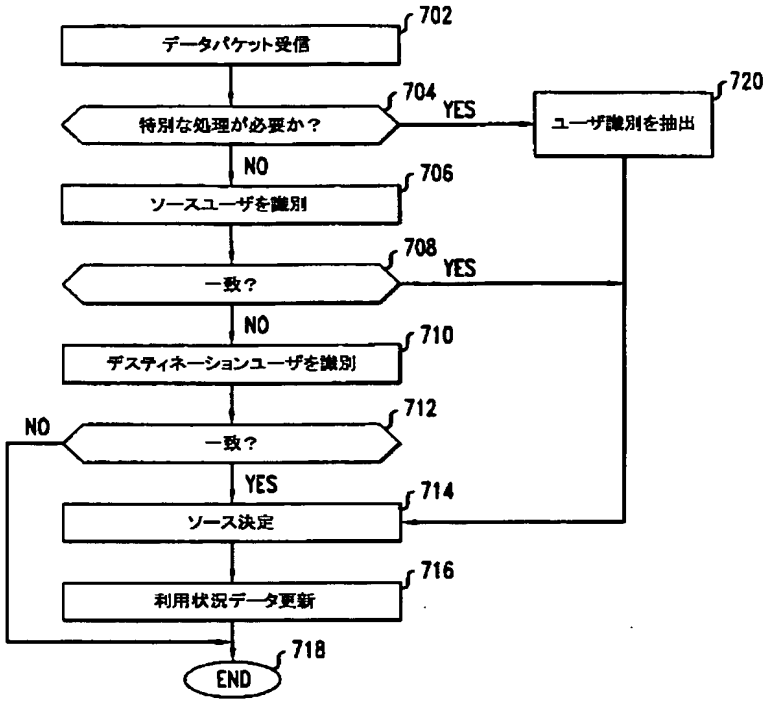
【図５】


502
504
506
508
IP-ADDR
マスク
PROTO
ポート範囲

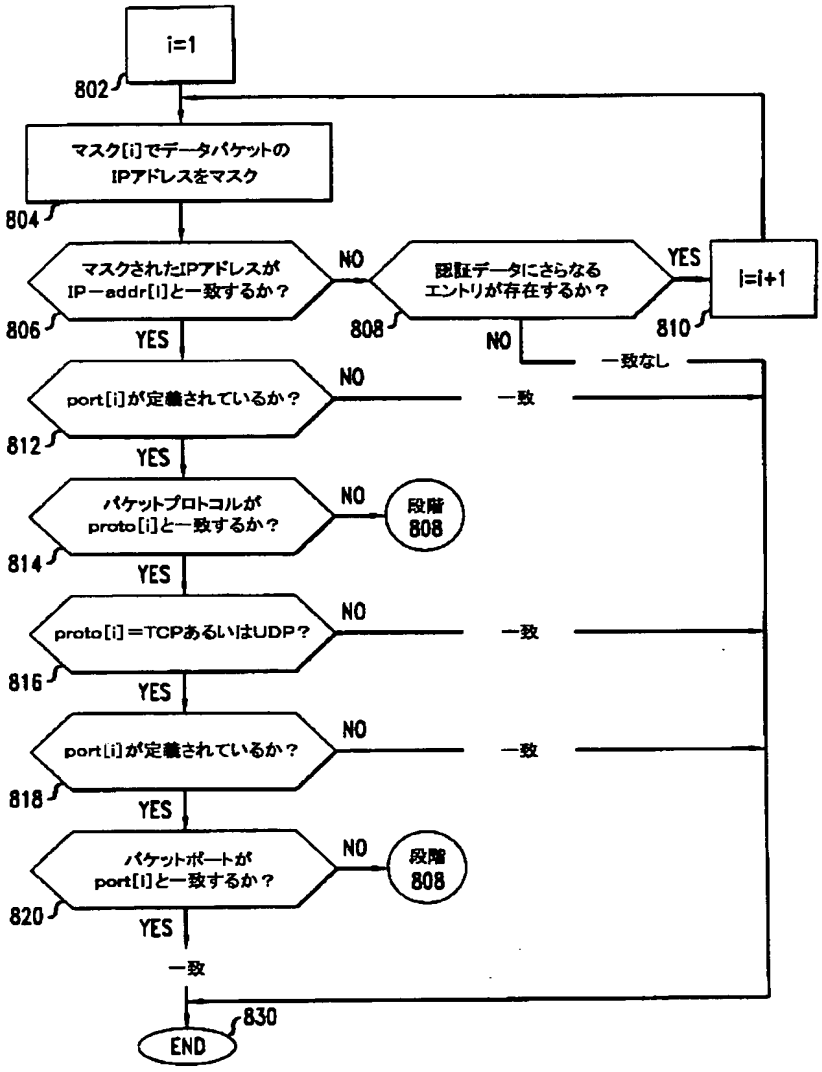
【図６】


IPデータグラム
TCPセグメント
600
602
604
606
IPヘッダ
TCPヘッダ
TCPデータ
ソースポート
デスティネーションポート
614
616
608
610
612
プロトコル
ソースIPアドレス
デスティネーションIPアドレス

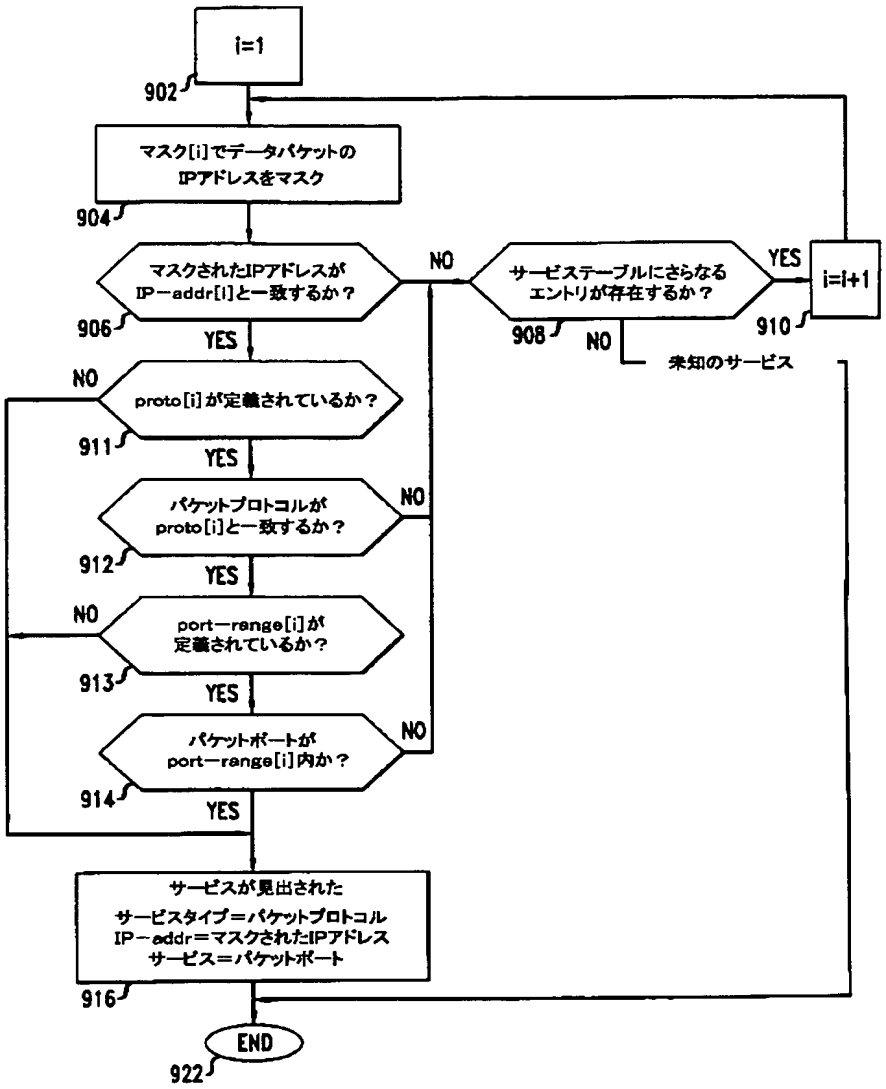
【図７】


702
データパケット受信
704
特別な処理が必要か？
YES
720
ユーザ識別を抽出
NO
706
ソースユーザを識別
708
一致？
YES
NO
710
デスティネーションユーザを識別
712
NO
一致？
YES
714
ソース決定
716
利用状況データ更新
718
END

【図８】


i=1
802
マスク[i]でデータパケットの
IPアドレスをマスク
804
マスクされたIPアドレスが
IP－addr[i]と一致するか？
806
NO
YES
認証データにさらなる
エントリが存在するか？
808
YES
i=i+1
810
NO
一致なし
port[i]が定義されているか？
812
NO
一致
YES
パケットプロトコルが
proto[i]と一致するか？
814
NO
段階
808
YES
proto[i]＝TCPあるいはUDP？
816
NO
一致
YES
port[i]が定義されているか？
818
NO
一致
YES
パケットポートが
port[i]と一致するか？
820
NO
段階
808
YES
一致
830
END

【図９】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	テーマコード（参考）
Ｇ０６Ｆ　15/177	６７２	Ｇ０６Ｆ　15/177	６７２Ｃ
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ａ

(71) 出願人　596077259
600 Mountain Avenue, Murray Hill, New Jersey 07974－0636U. S. A.
(72) 発明者　ステファン　マイケル　ブロット
アメリカ合衆国、07901　ニュージャージー、ジレット、ロング　ヒル　ロード　384
(72) 発明者　ユリ　ブライトバート
アメリカ合衆国、07940　ニュージャージー、マディソン、フェアーファックス　コート　90
(72) 発明者　クリフォード　イー．マーチン
アメリカ合衆国、08836　ニュージャージー、マーチンスビル、エヌ．ボッセラー　アベニュー　802

拒絶理由通知書

特許出願の番号	特願２０００－０５０４７６
起案日	平成１５年　８月　７日
特許庁審査官	小林　紀和　４２４０　５Ｘ００
特許出願人代理人	丸山　隆夫　様
適用条文	第２９条の２

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

この出願の請求項　１－１４　に係る発明は、その出願の日前の出願であって、その出願後に出願公開された下記　１，２　の出願の願書に最初に添付した明細書又は図面に記載された発明と同一であり、しかも、この出願の発明者がその出願前の出願に係る上記の発明をした者と同一ではなく、またこの出願の時において、その出願人がその出願前の出願に係る上記特許出願の出願人と同一でもないので、特許法第２９条の２の規定により特許を受けることができない。

記

１.特願２０００－１４８６８４号（特開２００１－４４９９２号）
２.特願平１０－２３２４４０号（特開２０００－０６９０１７号）
（備考）
引例１の段落１２，１３、図１を参照。
引例２の請求項１を参照。

先行技術文献調査結果の記録

・調査した技術分野
国際特許分類第７版（IPC 7）: H04L 12/
Ｆタームテーマ　：　5K030（広域データ交換）

この拒絶理由通知書の内容等に関する問い合わせ先
特許審査第四部　デジタル通信（データネットワーク）小林紀和
電話　(03) 3581-1101 内線3556